中華民國專利公報 [19] [12]

[11]公告編號：401562
[44]中華民國 89年 (2000) 08月11日
發明

全 7 頁

[51] Int.Cl 06: G06F9/44

[54]名 稱：預防非法寫入至一受保護之非揮發性儲存體之方法及裝置

[21]申請案號：086101163 [22]申請日期：中華民國 86年 (1997) 01月31日

[72]發明人：
馬克艾伯奇 美國
法蘭克威德若比 美國
[71]申請人：
英特爾公司 美國加州九五〇五二－八一一九聖達克拉市米遜學院大道二二〇〇號
[74]代理人：陳長文 先生

1

[57]申請專利範圍：

1. 一種用於保護非揮發性儲存體不會受到非法寫入之電腦建構的方法，該種方法是用於一包含一受保護之非揮發性儲存體的電腦系統，該種方法包含下列步驟：

a)保護電腦系統之多個驗證功能，該等驗證功能是配備成為利用一相關於寫入資料之電子簽名來驗證寫入至非揮發性儲存體之寫入資料，該電子簽名之內容在功能上決定於寫入資料之內容；

b)啟動該等驗證功能以驗證每一寫入至非揮發性儲存體的寫入資料，及只允許經驗證之寫入資料寫入至受保護之非揮發性儲存體。

2.根據申請專利範圍第1項之該電腦建構的方法，其中步驟(a)包含儲存該等驗證功能於電腦系統之記憶體的一受保護部份。

2

3.根據申請專利範圍第2項之該電腦建構的方法，其中步驟(a)之該等驗證功能是建構成為電腦系統之多個系統基本輸入／輸出服務(BIOS)；且步驟(a)包含在系統啟始期間拷貝該等多個系統BIOS進入電腦系統之系統管理記憶體，系統管理記憶體通常未對映至電腦系統之一正常系統記憶體空間，除了當電腦系統是在系統管理模式之下執行時以外，且無法寫入該系統管理記憶體，除了系統啟始及系統執行模式轉變以外。

4.根據申請專利範圍第1項之該電腦建構的方法，其中相關之電子簽名是藉由利用一秘密私鑰以加密第一摘要來產生，而第一摘要是基於寫入之寫入資料之內容來產生；且步驟(b)包含：

(b.1)啟動受保護之驗證功能之一受保護的解密功能以藉由利用一受保護之公鑰

以解密相關之電子簽名來重建第一摘要，而該公鑰與該秘密私鑰形成互補；

(b.2)啟動受保護之驗證功能之一受保護的訊息摘要功能以基於該寫入之寫入資料的內容來產生第二摘要；及

(b.3)啟動受保護之驗證功能之一受保護的摘要比較功能以藉由比較第一與第二摘要來決定是否該寫入之寫入資料是真實的。

5. 根據申請專利範圍第4項之該電腦建構的方法，其中步驟(b)進一步包含步驟(b.4)，而步驟(b.4)有條件地啟動受保護之驗證功能之一受保護的拷貝設施以拷貝該寫入資料進入受保護之非揮發性儲存體，如果在步驟(b.3)中第一及第二摘要通過比較測試的話。

6. 一種電腦系統，該種電腦系統包含：

(a)一非揮發性儲存體；

(b)多個用以在運作期間驗證寫入至非揮發性儲存體之寫入資料的驗證功能，該等驗證功能利用一相關於該寫入資料之電子簽名來驗證該寫入資料，該電子簽名之內容在功能上決定於該寫入資料的內容；

(c)一用以在運作期間儲存及保護該等多個驗證功能之受保護之記憶體單元；及

(d)一耦接至非揮發性儲存體及受保護之記憶體單元的處理器，該處理器是用以在運作期間啟動驗證功能以驗證每一寫入至非揮發性儲存體之寫入資料，及只允許經驗證之寫入資料寫入至非揮發性儲存體。

7. 根據申請專利範圍第6項之電腦系統，其中該等多個驗證功能包含：

一藉由利用一公鑰以解密電子簽名來重建第一摘要之解密功能，而該電子簽名是藉由利用一秘密私鑰以一互補方式加密第一摘要來產生；

一用以基於該寫入之寫入資料的內容以相同於產生第一摘要之方式來產生第二摘要的訊息摘要功能；及

一藉由比較第一與第二摘要來決定是否該寫入之寫入資料是真實之摘要比較功能。

8. 根據申請專利範圍第7項之電腦系統，其中解密功能，訊息摘要功能與摘要比較功能是建構成為電腦系統之多個系統基本輸入／輸出服務(BIOS)，該等系統輸入／輸出服務是在系統啟始期間拷貝進入受保護之記憶體單元，受保護之記憶體單元通常未對映至電腦系統之一正常系統記憶體空間，除了當處理器是在系統管理模式之下執行時以外，且無法寫入受保護之記憶體單元，除了系統啟始及系統執行模式轉變以外。

9. 根據申請專利範圍第8項之電腦系統，其中

非揮發性儲存體是一用以儲存系統BIOS之FLASH記憶體儲存單元；

解密功能，訊息摘要功能，摘要加密功能與公鑰預先儲存於FLASH記憶體儲存單元；

電腦系統進一步包含耦接至處理器之主記憶體；且

寫入之寫入資料是儲存於主記憶體之一緩衝器的系統BIOS更新

10. 根據申請專利範圍第9項之電腦系統，其中

電腦系統進一步包含一耦接至處理器，主記憶體，受保護之記憶體單元與FLASH記憶體以控制記憶體存取的記憶體控制器；

一耦接至記憶體控制器與FLASH記憶體以審核記憶體控制器提供給FLASH記憶體以進行寫入之一寫入訊號，及產生一中斷以使處理器處於系統管理模式的FLASH保護電路。

11. 根據申請專利範圍第10項之電腦系統，其中

電腦系統進一步包含一耦接至處理器與FLASH保護電路以通知該寫入給FLASH保護電路之輸入／輸出埠。

12. 根據申請專利範圍第7項之電腦系統，其中該等多個驗證功能進一步包含一拷貝功能，而該拷貝功能是用以有條件地拷貝該寫入之寫入資料進入非揮發性儲存體，如果第一與第二摘要通過摘要比較功能之比較的話。

13. 一種電腦系統母板，該種電腦系統母板包含：

(a)一非揮發性記憶體儲存單元；及

(b)儲存於該非揮發性記憶體儲存單元之系統基本輸入／輸出服務(BIOS)，該BIOS包含多個用以驗證在電腦系統之運作期間進入非揮發性儲存單元之寫入資料的驗證功能，且該非揮發性儲存單元與電腦系統母板整合，該驗證功能利用一相關於該等系統BIOS更新之電子簽名來驗證該等系統BIOS更新，該電子簽名之內容在功能上決定於該等系統BIOS更新之內容。

14. 根據申請專利範圍第13項之電腦系統母板，其中電腦系統母板進一步包含：

(c)用以儲存系統BIOS更新於一緩衝器之主記憶體。

15. 根據申請專利範圍第14項之電腦系統母板，其中電腦系統母板進一步包含：

(d)用以在電腦系統之運作期間儲存及保護該等多個驗證功能之系統管理記憶體，該等多個驗證功能是在系統啟始期間拷貝進入系統管理記憶體，系統管理記憶體通常未對映至電腦系統之一正常系統記憶體空間，除了當電腦系統是在系統管理模式之下執行時以外，且無法寫入該系統管理記憶體，除了系統啟始及系統執行模式轉變以外。

16. 根據申請專利範圍第15項之電腦系統母板，其中電腦系統母板進一步包含：

(e)一耦接至非揮發性記憶體儲存體及

系統管理記憶體的處理器，該處理器是用以在處於系統管理模式之電腦系統之運作期間啟動驗證功能以驗證系統BIOS更新，及只允許經驗證之系統BIOS更新自主記憶體之緩衝器寫入至非揮發性記憶體儲存單元。

17. 根據申請專利範圍第16項之電腦系統母板，其中電腦系統母板進一步包含：

(f)一耦接至處理器，主記憶體，系統管理記憶體及非揮發性記憶體儲存單元以控制記憶體存取的記憶體控制器；

(g)一耦接至記憶體控制器與非揮發性記憶體儲存單元以審核記憶體控制器提供給非揮發性記憶體儲存單元以進行寫入之一寫入訊號，該寫入訊號受到啟始以寫入系統BIOS更新於非揮發性記憶體儲存單元，及產生一中斷以使電腦系統處於系統管理模式的非揮發性記憶體存取保護電路。

18. 根據申請專利範圍第17項之電腦系統母板，其中電腦系統母板進一步包含：

一耦接至處理器與非揮發性記憶體存取保護電路以通知該寫入給非揮發性記憶體保護電路之輸入／輸出埠。

19. 根據申請專利範圍第13項之電腦系統母板，其中該等多個驗證功能包含：

一藉由利用一公鑰以解密電子簽名來重建第一摘要之解密功能，該電子簽名是藉由利用一秘密私鑰以一互補方式加密第一摘要來產生；

一用以基於系統BIOS更新的內容以相同於產生第一摘要之方式來產生第二摘要的訊息摘要功能；及

一藉由比較第一與第二摘要來決定是否系統BIOS更新是真實之摘要比較功能。

20. 根據申請專利範圍第19項之電腦系統母板，其中該等多個驗證功能進一步包含一拷貝功能，而該拷貝功能是用以有條件地拷貝該等系統BIOS更新進入非

揮發性記憶體儲存單元，如果第一與第二摘要通過摘要比較功能之比較的話。

圖式簡單說明：

第一圖－第二圖展示本發明之基本組件與該等組件之相互關係；

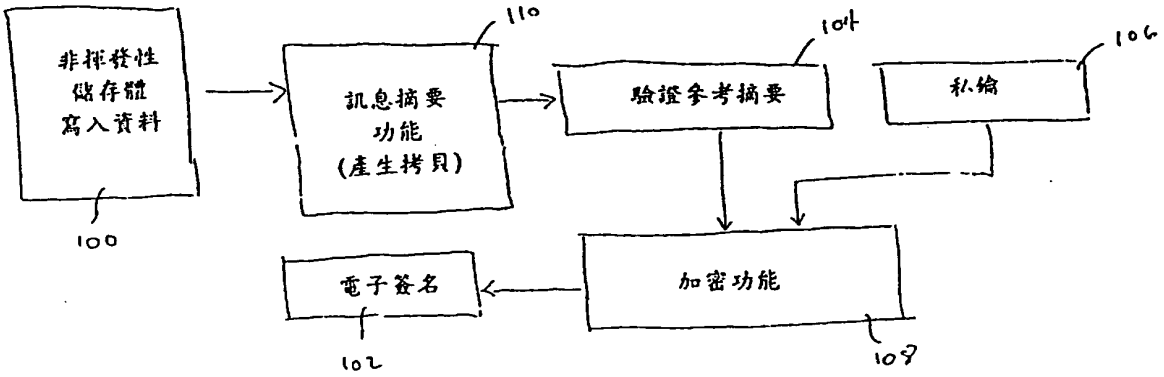
第三圖展示一融入本發明對於保護驗證功能之說明的示範電腦系統；

第四圖更詳細展示示範電腦系統之系統BIOS，與針對一實例，作業系統；

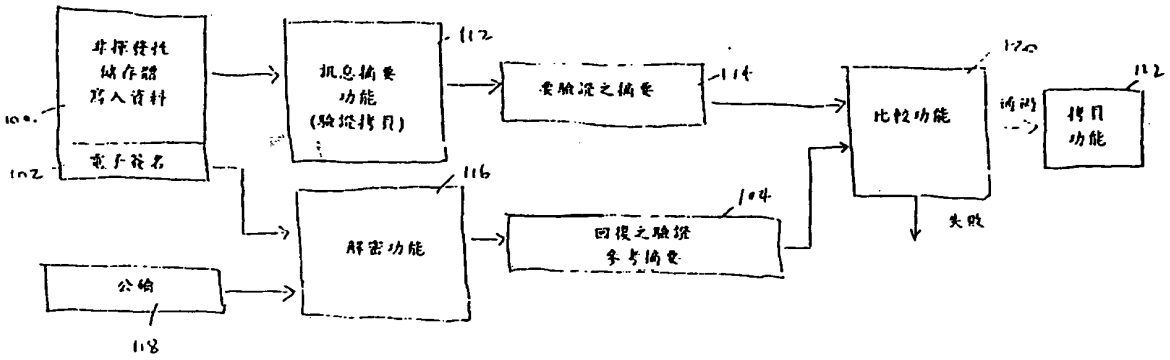
第五圖更詳細展示第二圖之FLASH保護電路；

第六圖展示在一系統管理模式下之示範電腦系統的執行流程；

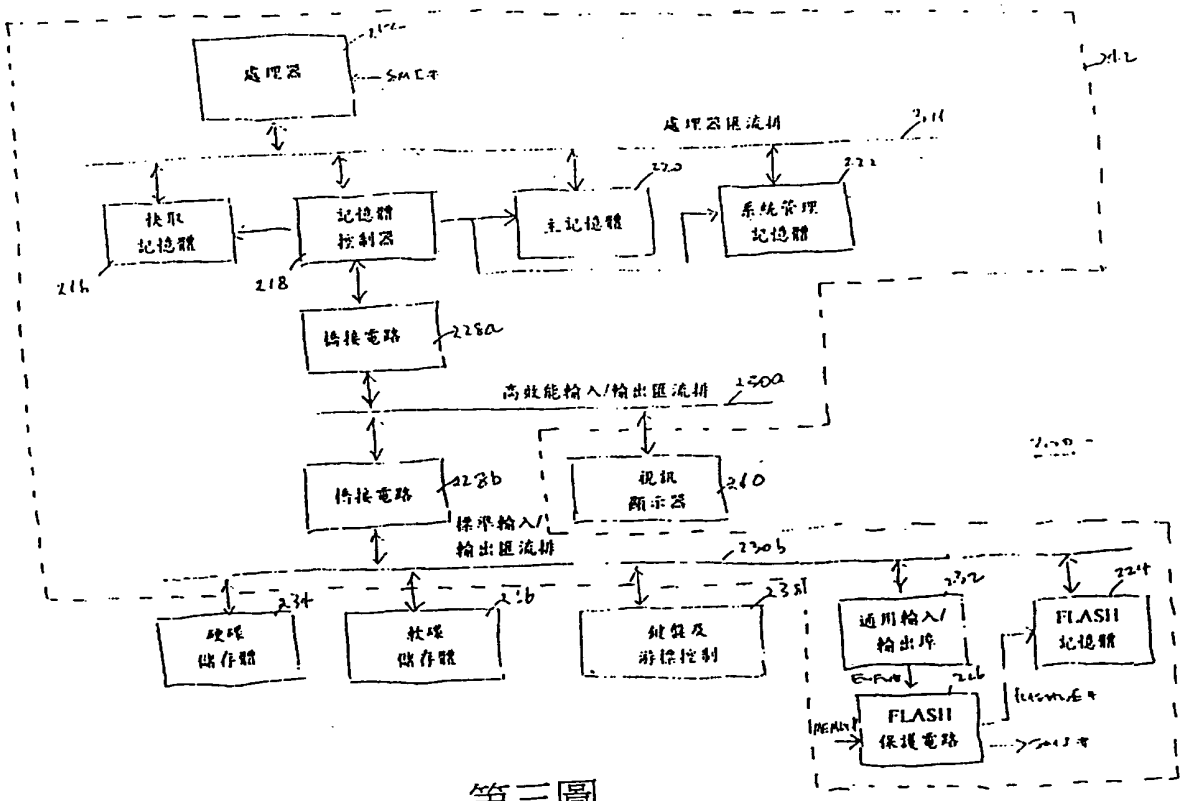
第七圖展示一用以寫入FLASH記憶體之執行流程的實例。



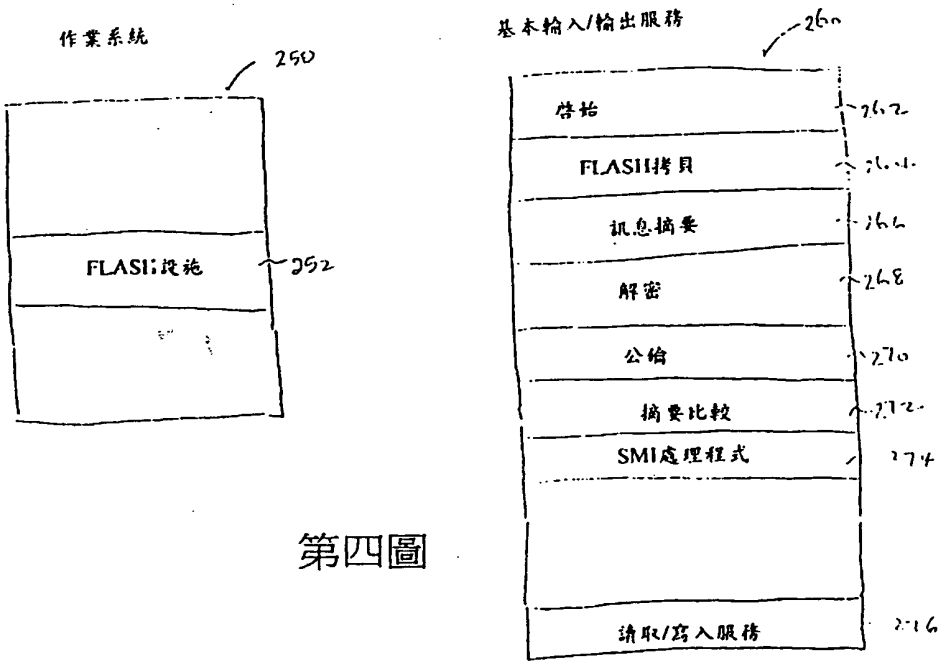
第一圖



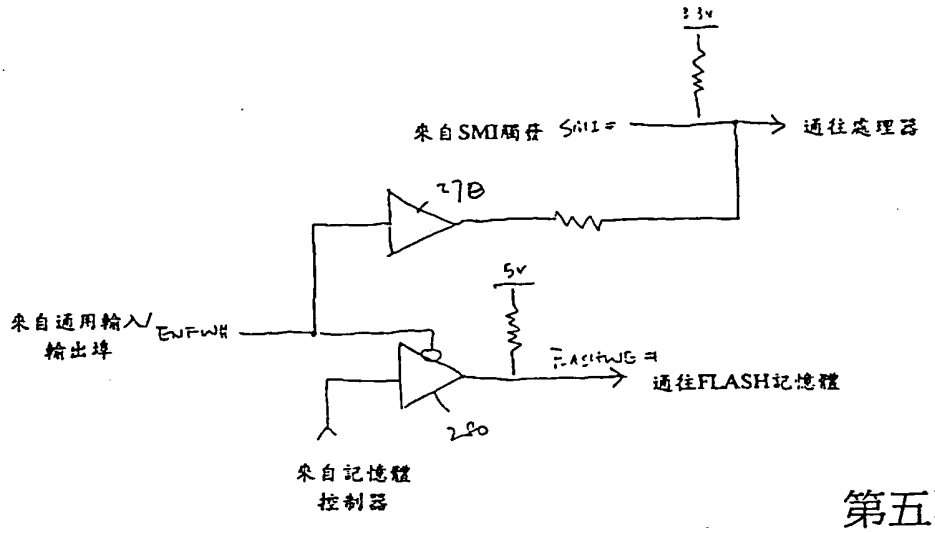
第二圖


處理器
處理器匯流排
快取記憶體
記憶體控制器
主記憶體
系統管理記憶體
橋接電路
高效能輸入/輸出匯流排
橋接電路
視訊顯示器
標準輸入/輸出匯流排
硬碟儲存體
軟碟儲存體
鍵盤及游標控制
通用輸入/輸出埠
FLASH記憶體
FLASH保護電路

第三圖

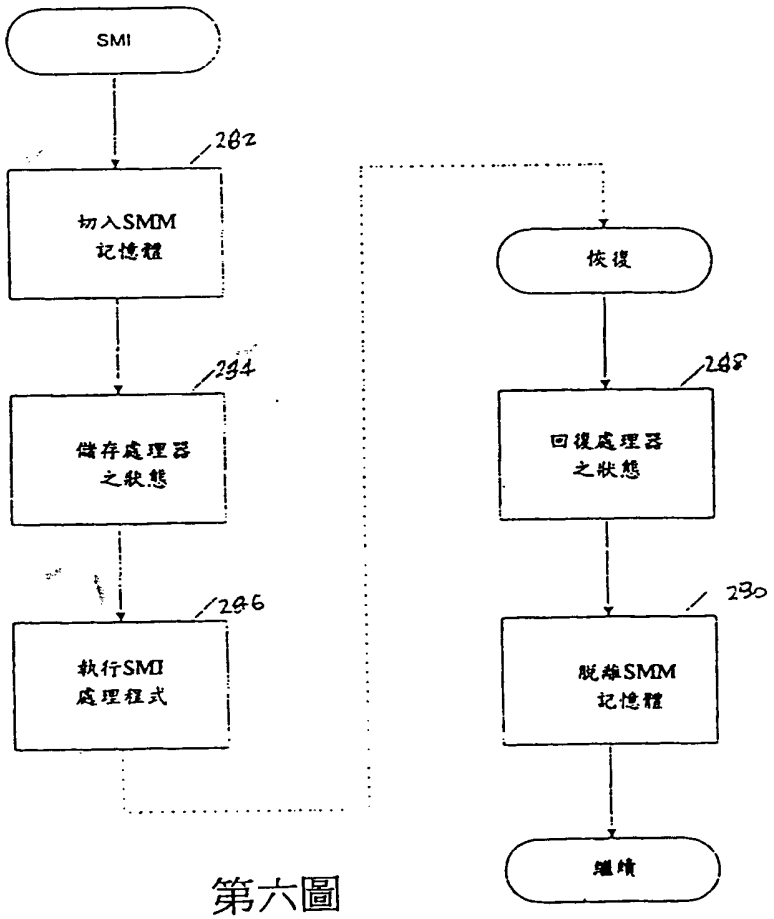

作業系統
250
FLASH設施
252
基本輸入/輸出服務
260
啓始
FLASH拷貝
訊息摘要
解密
公鑰
摘要比較
SMI處理程式
讀取/寫入服務

第四圖

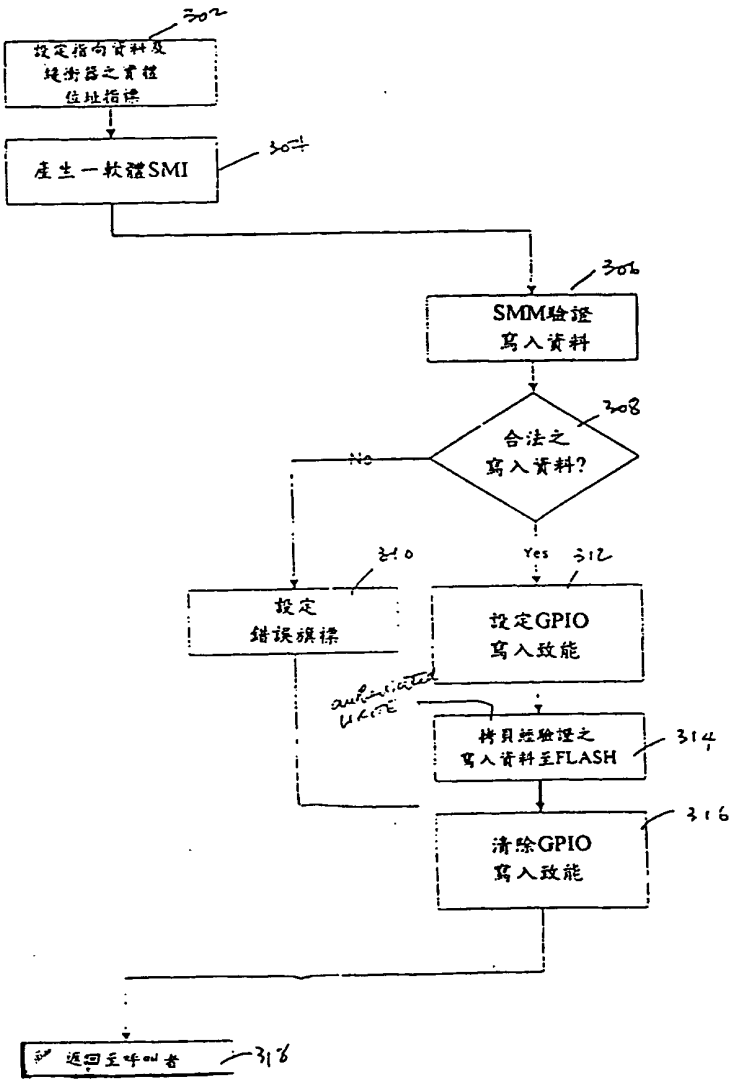


第五圖

系統管理模式(以前技術)



第六圖


302
設定指向資料及
儲存器之實體
位址指標
304
產生一軟體SMI
306
SMM驗證
寫入資料
308
合法之
寫入資料?
No
Yes
310
設定
錯誤旗標
312
設定GPIO
寫入致能
Automatically
clear
314
將資料驗證之
寫入資料至FLASH
316
清除GPIO
寫入致能
318
返回至呼叫者

第七圖

Methods And Apparatus For Preventing Unauthorized Write Access To A Protected Non-volatile Storage

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of computer systems. More specifically, the present invention relates to data security on computer systems.

2. Background Information

Existing methods of preventing unauthorized write access to non-volatile storage such as FLASH memory typically rely on "secret" access methods to a write enable circuit. These "secret" access methods to the write enable circuit can be reverse-engineered through the use of standard debugging hardware. Once reverse engineered, a person will be able to produce code that can write to the "protected" non-volatile storage at will. If the code is used in a malicious manner, it can be used to introduce viruses into the "protected" non-volatile storage or even destroy the content of the non-volatile storage.

Thus, it is desirable to have a more robust approach to preventing unauthorized access to non-volatile storage, in particular, an approach that does not rely on the access method not being known. As will be described in more detail below, the present invention achieves these and other desirable results.

SUMMARY OF THE INVENTION

In accordance to the present invention, an electronic signature is generated in a predetermined manner and attached to a transferable unit of write data, to facilitate authenticating the write data before allowing the write data to be written into a protected non-volatile storage. The write data is authenticated using a collection of secured authentication functions. Additionally, the actual writing of the authenticated write data into the protected non-volatile storage is performed by a secured copy utility.

The electronic signature is functionally dependent on the content of the write data, and the predetermined manner of generating the electronic signature is reproducible during write time. In one embodiment, the electronic signature is generated by the creator of the write data, by generating a digest based on the content of the write data using a message digest function, and then encrypting the generated digest with a secret private key using an encryption function.

The collection of secured authentication functions include a secured corresponding copy of the message digest function, and a secured complementary decryption function. During operation, the secured decryption function reconstitutes the original digest by decrypting the electronic signature with a secured complementary public key, while the secured copy of the message digest function generates another digest based on the content of the write data to be authenticated. The two digests are compared using a secured comparison function. If the two digests pass the comparison, the secured copy utility is invoked to copy

the authenticated write data into the protected non-volatile storage, otherwise, the write data are rejected.

In one embodiment, the authentication functions are secured by copying them into a normally unavailable system management memory during system initialization. The authentication functions are invoked using a system management interrupt (SMI), which when asserted, automatically maps the system management memory into the normal system memory space. A non-volatile memory write security circuitry is provided to qualify a memory write signal provided to the protected non-volatile storage, and to generate the SMI whenever a write to the protected non-volatile storage is requested.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figures 1 - 2 illustrate the essential elements of the present invention, and their interrelationships with each other;

Figure 3 illustrates an exemplary computer system incorporated with the teachings of the present invention on securing the authentication functions;

Figure 4 illustrates the system BIOS, and for one embodiment, the operating system of the exemplary computer system in further detail;

Figure 5 illustrates the FLASH security circuitry of Figure 3 in further detail;

Figure 6 illustrates execution flow of the exemplary computer system under a system management mode; and

Figure 7 illustrates one embodiment of the execution flow for writing into FLASH memory.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, for purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention. Furthermore, for ease of understanding, certain method steps are delineated as separate steps, however, these separately delineated steps should not be construed as necessarily order dependent in their performance.

Referring now to Figures 1 and 2, two block diagrams illustrating the essential elements of the present invention, and their interrelationships to each other are shown. As illustrated, a transferable unit of non-volatile storage write data 100 is provided with an electronic signature 102 to facilitate authenticating write data 100 prior to allowing write data 100 to be written into a non-volatile storage. Preferably, electronic signature 102 is "attached" to write data 100. Examples of a transferable unit include a file, or a block, whereas examples of non-volatile storage include FLASH memory or erasable programmable read-only-memory (EPROM). Examples of write data is system basic input/output service (BIOS) updates, such as additions, deletions and modifications. For many applications, it is expected that electronic signature 102 is generated and "attached" to write data 100 at the time write data 100 is created.

For the illustrated embodiment, electronic signature 102 is generated by encrypting a reference digest 104 with a secret private key 106 using an encryption

function 108. The reference digest 104 is generated using a message digest function 110. In other words, the content of reference digest 104 is functionally dependent on the content of write data 100. Accordingly, the content of electronic signature 102 is also functionally dependent on the content of write data 100.

At write time, a secured corresponding copy of message digest function 112 generates a "new" digest 114 in real time. At the same time, a secured complementary decryption function 116 reconstitutes original reference digest 104 by decrypting electronic signature 102 using secured complementary public key 118. The two digests 104 and 114 are provided to a secured comparison function 120 to determine if they are identical. The two digests 104 and 114 are identical if write data 100 is authentic, since both digests 104 and 114 are functionally dependent on the contents of write data 100, generated by copies of the same message digest function 110 and 112, and the encryption were decrypted in a complementary manner. If the two digests 104 and 114 compared successfully, a secured copy function 122 is notified to perform the actual writing into the protected non-volatile storage, otherwise the write data is rejected.

Encryption and decryption functions 108 and 116 may implement any one of a number of private/public key encryption/decryption techniques known in the art. Similarly, message digest function 110/112 may also implement any one of a number of message digest techniques known in the art. For further information on private/public key encryption/decryption techniques, see e.g. Hellman et al., Public Key Cryptographic Apparatus and Method, US Patent 4,218,582, and Rivest et al., Cryptographic Communications System and Method, US Patent 4,405,829; and for further information on message digest, see e.g. Method for Identifying Subscribers

and for Generating and Verifying Electronic Signatures in a Data Exchange System, US Patent 4,995,082, and Rivest, The MD5 Message Digest Algorithm, Request For Comment (RFC) 1321, Apr. 1992.

Creation of electronic signature 102 and associating it with write data 100 as described above, may be practiced in any number of computer systems known in the art, provided they are equipped to store and execute message digest function 110 and encryption function 108. It is anticipated that for most applications, creation of electronic signature 102 will be practiced on the same computer system where write data 100 is created. For example, for the above mentioned system BIOS update application, it is anticipated that the system BIOS updates and electronic signature 102 will be generated and associated at the same time and on the same computer system.

Figure 3 illustrates an exemplary computer system 200 incorporated with the teachings of the present invention on authenticating write data before allowing the write data to be written into a protected non-volatile storage. Exemplary computer system 200 includes processor 212, processor bus 214, cache memory 216, memory controller 218, and a plurality of other memory units 220 - 224 coupled to each other as shown. Other memory units 220 - 224 include main memory 220, system management memory 222, and FLASH memory 224. In accordance to the present invention, exemplary computer system 200 includes in particular FLASH security circuitry 226. Additionally, computer system 200 includes bridge circuits 228a - 228b, high performance and standard (input/output) I/O buses 230a - 230b, general purpose I/O (GPIO) ports 232, hard and diskette

storages 234 - 236, keyboard and cursor control device 238, and display 240, coupled to each other and the above enumerated elements as shown.

For the illustrated embodiment, buses 214, 230a and 230b are disposed on motherboard 242. Elements 212, 216 - 226, 228a - 228b and 232 are either removably interconnected to motherboard 242 via sockets (not shown) or "soldered" onto motherboard 242, whereas elements 234 - 238 are coupled to motherboard 42 through cables and connectors (not shown).

Processor 212 performs the conventional function of executing code. Processor 212 is equipped to execute code in multiple modes including a system management mode (SMM). Processor 212 is also equipped to respond to a wide variety of interrupts including a system management interrupt (SMI), which places processor 212 in SMM. Memory controller 218 and volatile memory units 216, 220 and 222 perform the conventional functions of controlling memory access, and providing execution time storage respectively. In particular, for each write access to memory, memory controller 218 generates a MEMW# signal for the addressed memory unit. Memory controller 218 normally does not map system management memory 222 as part of the normal system memory space. System management memory 222 is mapped into the system memory space, when processor 212 enters SMM. Furthermore, except for system initialization, processor mode transition, and execution in SMM, system management memory 222 is write disabled.

FLASH memory 224 performs its conventional function of providing non-volatile storage respectively. In particular, FLASH memory 224 stores system BIOS. During system initialization, the bulk of the system BIOS that are not security

sensitive are loaded into main memory 220, whereas the remaining system BIOS (including in particular the write data authentication functions) that are security sensitive are loaded into system management memory 224. Flash security circuit 226 protects FLASH memory 224 from unauthorized write accesses, by keeping FLASH memory 224 write disabled, and generating an SMI to invoke the secured system BIOS write data authentication functions in system management memory 222 to authenticate the write data, whenever it enables FLASH memory 224 for a write access. General purpose I/O ports 232 also perform their conventional functions for providing I/O ports to a variety of peripherals. In particular, one of the I/O ports is used to notify FLASH security circuit 226 of a write request to FLASH memory 224. The write request is denoted by writing to a corresponding register of the I/O port using a standard I/O instruction of exemplary computer system 200.

Hard disk storage 234 also performs the conventional function of providing non-volatile storage. In particular, hard disk storage 234 stores operating system of exemplary computer system 200. During system initialization, operating system is loaded into main memory 220. All other elements perform their conventional function known in the art. Except for the particularized functions and/or requirements, all enumerated elements are intended to represent a broad category of these elements found in computer systems.

Figure 4 illustrates system BIOS and operating system of exemplary computer system 200 in further detail. As shown, system BIOS 260 includes init function 262, FLASH copy utility 264, message digest function 266, decryption function 268, public key 270, digest comparison function 272, SMI handler 274 and

read/write service 276, whereas, for some embodiments, operating system 250 includes FLASH utility 252.

Init function 262 initializes system BIOS 260 during system initialization, including loading FLASH copy utility 264, message digest function 266, decryption function 268, public key 270, digest comparison function 272, and SMI handler 274 into system management memory 222. As described earlier, system management memory 222 is normally not mapped into system management space, unless a SMI is triggered placing processor 212 in SMM, and system management memory 222 is write disabled except for initialization, processor mode transition, and execution in SMM. Accordingly, these system BIOS functions are secured from malicious modification.

SMI handler 274 services SMIs, invoking other functions (including the write data authentication functions) as necessary, depending on the cause of a particular SMI. As will be described in more detail below, SMI handler 274 is given control upon entry into SMM. As described earlier, message digest 266 generates a digest in real time for the write data of a FLASH write request, in accordance to the content of the write data, and decryption function 268 decrypts the electronic signature "attached" to the write data of the FLASH write request using public key 270, to reconstitute the FLASH write data's original digest. Digest comparison function 272 compares the two digests, and finally FLASH copy utility 264 performs the actual writing of the authenticated data into FLASH memory 224. Message digest function 266, decryption function 268, digest comparison function 272, and FLASH copy utility 264 are invoked in due course by SMI handler 274 upon determining that a SMI is triggered by FLASH security circuitry 226.

Read/Write services 276 provides read and write services to I/O devices. Read/Write services 276 are among the bulk of the BIOS functions that are loaded into main memory 220 during system start up.

For some embodiments, FLASH utility 252 is included to perform various FLASH related functions including in particular copying of FLASH write data from an external source medium to a buffer in main memory 220, and then copying the FLASH write data from the buffer into FLASH memory 224 by way of read/write services 276, which invokes message digest function 266, decryption function 268, etc., to validate the FLASH write data, and if validated, FLASH copy utility 264 to perform the actual writing, to be described more fully below. Examples of such FLASH write data are system BIOS additions, deletions, and modifications described earlier, and an example of an external source medium is a diskette.

Figure 5 illustrates FLASH security circuit 226 in further detail. As shown, FLASH security circuit 226 includes first and second drivers 278 and 280. The input (ENFW#) of first driver 278 is provided by one of the I/O ports of GPIO ports 232, whereas the output of first driver 278 is coupled to a signal line coupling a SMI trigger mechanism to processor 212. Thus, whenever, GPIO ports 232 sets ENFW# active to enable write access, in response to a FLASH write request, first driver 278 causes a SMI to be triggered for processor 212.

The inputs (ENFW# and MEMW#) of second driver 280 are provided by the same I/O port of general purpose I/O ports 232 and memory controller 218

respectively, whereas the output (FLASHWE#) of second driver 280 is provided to FLASH memory 224. FLASHWE# is tri-stated. FLASHWE# becomes active, when both MEMW# and ENFW# are active. In other words, the write signal (MEMW#) from memory controller 218 is qualified by ENFW#, which at the same time through first driver 278 would cause a SMI to be triggered. Thus, the secured authentication functions stored in system management memory 222 would be invoked to authenticate the write data before allowing them to be written into FLASH memory 224.

Figure 6 illustrates execution flow of the exemplary computer system in SMM. As shown, upon detection of an SMI, processor 212 directs memory controller 218 to switch in and map system management memory 222 as part of the system memory space, and in response, memory controller 218 performs the requested switching and mapping accordingly, step 282. Next, processor 212 saves the processor state into system management memory 222, step 284. Upon saving the processor state, processor 212 transfers execution control to pre-stored SMI handler 274, step 286.

SMI handler 274 then determines the cause of the SMI and services the SMI accordingly, invoking other routines such as the authentication functions as necessary. Upon servicing the SMI, SMI handler 274 executes a Resume instruction to transfer execution control back to the interrupted programs. In response, processor 212 restores the saved processor state from system management memory 222, step 288. Furthermore, processor 212 directs memory controller 218 to unmap system management memory 222 from the system memory space and switch out

system management memory 222. In response, memory controller 218 performs the requested unmapping and switching accordingly, step 290.

As a result, the SMI is serviced in a manner that is transparent to the executing operating system, subsystems as well as applications. In other words, an SMI is a transparent system service interrupt.

Figure 7 illustrates one embodiment of the execution flow for writing data into FLASH memory 224. As shown, in response to a write request from an application, such as FLASH utility 252 described earlier, read/write services 276 set up the physical address pointers to the write data, step 302. Next, for the illustrated embodiment, read/write services 276 generate a software SMI to enter SMM and to provide the SMI handler with the physical address pointers of the write data, step 304. A software SMI is used and preferred at this point in time as opposed to the designated GPIO port 232 because FLASH memory would remain disabled during the authentication process.

Upon entry into SMM, as described earlier, SMI handler 274 is given control. Upon ascertaining the reason for the SMI, SMI handler 274 invokes message digest 266 and decryption function 268 to authenticate the write data identified by the physical address pointers, step 306. If the write data fails the authentication process, step 308, SMI handler 274 sets the appropriate error flags, step 310, clears the designated GPIO port, step 316, and exits SMM. Upon given control again, read/write services 276 returns to the caller, after performing the necessary "clean ups".

On the other hand, if at step 308, the write data passes the authentication process, SMI handler 274 enables write to FLASH memory 224, by setting the designated GPIO port 232, step 312. Once enabled, the authenticated write data are copied into FLASH memory 224, step 314. After all authenticated write data have been copied, as described earlier, SMI handler 274 clears the designated GPIO port 232, and exits SMM. Upon given control again, read/write services 276 returns to the caller, after performing the necessary "clean ups".

As described earlier, when SMI handler 274 enables write to FLASH memory 224 by way of the designated GPIO port, in addition to enabling FLASH memory 224 for write, a SMI is triggered. However, since this "new" SMI is triggered while the system is in SMM, the "new" SMI is discarded. The reason why the "new" SMI is triggered is because for the illustrated embodiment, the designated GPIO port 232 may be set outside SMM. The "automatic" SMI will ensure that the write data will be authenticated in the event that happens, preventing any possibility of bypassing the authentication process.

Thus, methods and apparatus for preventing unauthorized access to a protected non-volatile memory have been described. While the method and apparatus of the present invention has been described in terms of the above illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of restrictive on the present invention.

46371 HW
PG 8

ABSTRACT OF THE DISCLOSURE

An electronic signature is generated in a predetermined manner and attached to a transferable unit of write data, to facilitate authenticating the write data before allowing the write data to be written into a protected non-volatile storage. The write data is authenticated using a collection of secured authentication functions. Additionally, the actual writing of the authenticated write data into the protected non-volatile storage is performed by a secured copy utility.

第 86101163 號專利申請案
英文申請專利範圍修正本 (89 年 3 月)
ROC (Taiwan) Patent Application No. 86101163
Amended Claims (March 2000)

1. In a computer system comprising a protected non-volatile storage, a computer implemented method for protecting the non-volatile storage from unauthorized write access, the method comprising the steps of:

a) securing a plurality of authentication functions on the computer system, the authentication functions being equipped to authenticate write data of a write access to the non-volatile storage using an electronic signature associated with the write data, the content of the electronic signature being functionally dependent on the content of the write data;

b) invoking the authentication functions to authenticate write data of each write access to the non-volatile storage, and allowing only authenticated write data to be written into the protected non-volatile storage.

2. The computer implemented method as set forth in claim 1, wherein step (a) comprises securing the authentication functions in a secured portion of memory of the computer system.

3. The computer implemented method as set forth in claim 2, wherein the authentication functions of step (a) are implemented as a plurality of system basic input/output services (BIOS) of the computer system; and step (a) comprises copying the plurality of system BIOS into system management memory of the computer system during system initialization, the system management memory

being normally not mapped into a normal system memory space of the computer system except when the computer system is executing in a system management mode, and the system management memory being write protected except for system initialization and system execution mode transition.

4. The computer implemented method as set forth in claim 1, wherein the associated electronic signature is generated by encrypting a first digest with a secret private key, the first digest being generated based on the content of the write data of the write access; and step (b) comprises

(b.1) invoking a secured decryption function of the secured authentication functions to reconstitute the first digest by decrypting the associated electronic signature using a secured public key complementary to the secret private key,

(b.2) invoking a secured message digest function of the secured authentication functions to generate a second digest based on the content of the write data of the write access, and

(b.3) invoking a secured digest comparison function of the secured authentication functions to determine if the write data of the write access is authentic by comparing the first and second digests.

5. The computer implemented method as set forth in claim 4, wherein step (b) further comprises step (b.4) conditionally invoking a secured copy utility of the secured authentication functions to copy the write data into the protected non-volatile storage if the first and second digests compared successfully in step (b.3).

6. A computer system comprising:

(a) a non-volatile storage;

(b) a plurality of authentication functions for authenticating write data of a write access to the non-volatile storage during operation, the authentication functions authenticating the write data using an electronic signature associated with the write data, the content of the electronic signature being functionally dependent on the content of the write data;

(c) a secured memory unit for storing and securing the plurality of authentication functions during operation; and

(d) a processor coupled to the non-volatile storage and the secured memory unit for invoking the authentication functions during operation to authenticate write data of each write access to the non-volatile storage, and to allow only authenticated write data to be written into the non-volatile storage.

7. The computer system as set forth in claim 6, wherein the plurality of authentication functions include

a decryption function for reconstituting a first digest by decrypting the electronic signature with a public key, the electronic signature being generated by encrypting the first digest with a secret private key in a complementary manner,

a message digest function for generating a second digest based on the content of the write data of the write access in the same manner the first digest was generated, and

a digest comparison function for determining whether the write data of the write access is authentic by comparing the first and second digests.

8. The computer system as set forth in claim 7, wherein the decryption function, the message digest function and the digest comparison function are implemented as a plurality of system basic input/output services (BIOS) of the computer system,

which are copied into the secured memory unit during system initialization, the secured memory unit being normally not mapped into a normal system memory space of the computer system except when the processor is executing in a system management mode, and the secured memory unit being write protected except for system initialization and processor execution mode transition.

9. The computer system as set forth in claim 8, wherein

the non-volatile storage is a FLASH memory storage unit for storing system BIOS;

the decryption function, the message digest function, the digest encryption function and the public key are pre-stored in the FLASH memory storage unit;

the computer system further includes main memory coupled to the processor; and

the write data of the write access are system BIOS updates staged in a buffer in the main memory.

10. The computer system as set forth in claim 9, wherein

the computer system further includes a memory controller coupled to the processor, the main memory, the secured memory unit and the FLASH memory for controlling memory access;

a FLASH security circuit coupled to the memory controller and the FLASH memory for qualifying a write signal provided by the memory controller to the FLASH memory for the write access, and for generating an interrupt to place the processor in the system management mode.

11. The computer system as set forth in claim 10, wherein

the computer system further includes an I/O port coupled to the processor and the FLASH security circuit for notifying the FLASH security circuit of the write access.

12. The computer system as set forth in claim 7, wherein the plurality of authentication functions further include a copy function for conditionally copying the write data of the write access into the non-volatile storage if the digest comparison function successfully compares the first and second digests.

13. A computer system motherboard comprising:

(a) a non-volatile memory storage unit; and

(b) system basic input/output service (BIOS) stored in the non-volatile memory storage unit, the BIOS including a plurality of authentication functions for authenticating write data into the non-volatile storage unit during operation of a computer system integrated with the computer system motherboard, the authentication functions authenticating the system BIOS updates using an electronic signature associated with the system BIOS updates, the content of the electronic signature being functionally dependent on the content of the system BIOS updates.

14. The computer system motherboard as set forth in claim 13, wherein the computer system motherboard further includes

(c) main memory for staging the system BIOS updates in a buffer.

15. The computer system motherboard as set forth in claim 14, wherein the computer system motherboard further includes

(d) system management memory for storing and securing the plurality of authentication functions during operation of the computer system, the plurality of authentication functions being copied into the system management memory during system initialization, the system management memory being normally not mapped into a normal system memory space of the computer system except when the computer system is executing in a system management mode, and the system management memory being write protected except for system initialization and system execution mode transition..

16. The computer system motherboard as set forth in claim 15, wherein the computer system motherboard further comprises

(e) a processor coupled to the non-volatile memory storage and the system management memory for invoking the authentication functions during operation of the computer system in system management mode to authenticate the system BIOS updates, and to allow only authenticated system BIOS updates to be written from the buffer of main memory into the non-volatile memory storage unit.

17. The computer system motherboard as set forth in claim 16, wherein the computer system motherboard further comprises:

(f) a memory controller coupled to the processor, the main memory, the system management memory and the non-volatile memory storage unit for controlling memory access;

(g) a non-volatile memory access security circuit coupled to the memory controller and the non-volatile memory storage unit for qualifying a write signal provided by the memory controller to the non-volatile memory storage unit for a write access initiated to write the system BIOS updates into the non-volatile memory

storage unit, and for generating an interrupt to place the computer system in the system management mode.

18. The computer system motherboard as set forth in claim 17, wherein the computer system motherboard further includes an I/O port coupled to the processor and the non-volatile memory access security circuit for notifying the non-volatile memory security circuit of the write access.

19. The computer system motherboard as set forth in claim 13, wherein the plurality of authentication functions include

a decryption function for reconstituting a first digest by decrypting the electronic signature with a public key, the electronic signature being generated by encrypting the first digest with a secret private key in a complementary manner,

a message digest function for generating a second digest based on the content of the system BIOS updates in the same manner the first digest was generated, and

a digest comparison function for determining whether the system BIOS updates are authentic by comparing the first and second digests.

20. The computer system motherboard as set forth in claim 19, wherein the plurality of authentication functions further include a copy function for conditionally copying the system BIOS updates into the non-volatile memory storage unit if the digest comparison function successfully compares the first and second digests.

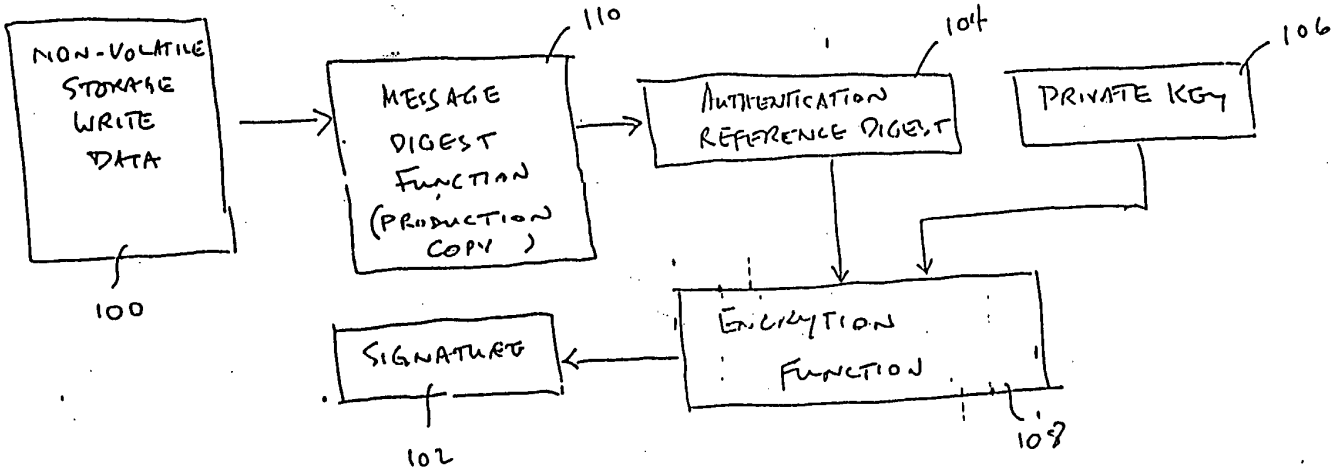


FIGURE 1

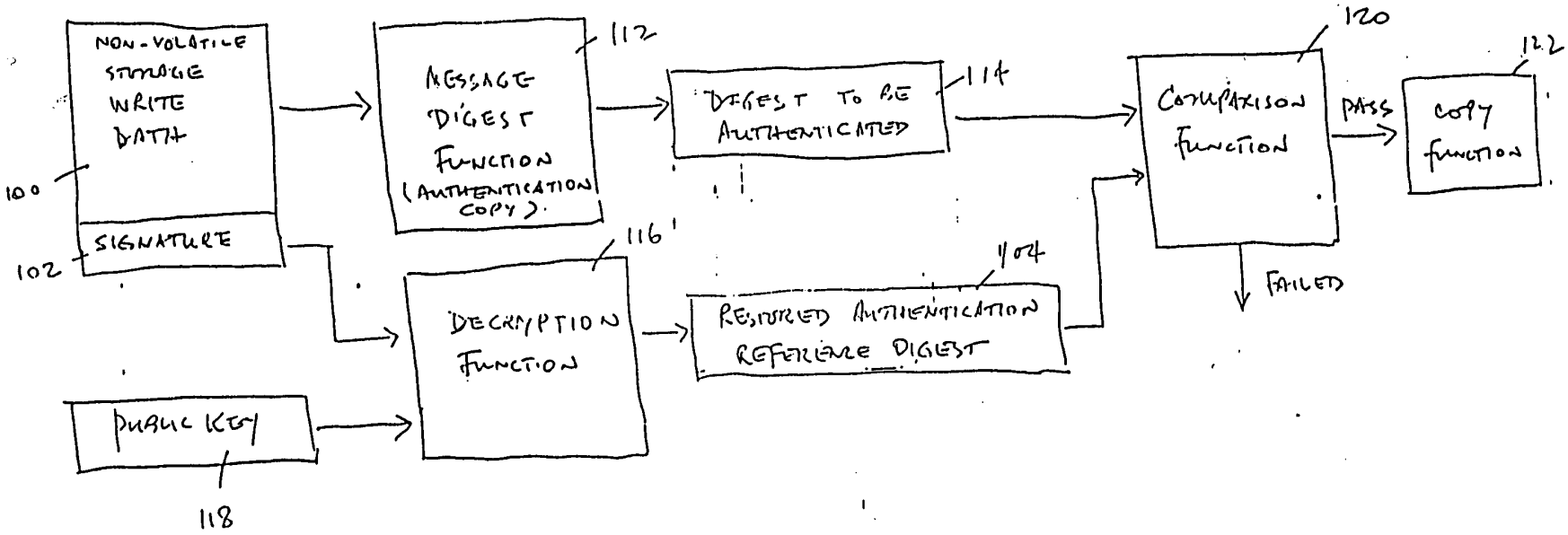

NON-VOLATILE STORAGE WRITE PATH
100
SIGNATURE
102
MESSAGE DIGEST FUNCTION (AUTHENTICATION COPY)
112
DIGEST TO BE AUTHENTICATED
114
DECRYPTION FUNCTION
116
PUBLIC KEY
118
RESTORED AUTHENTICATION REFERENCE DIGEST
104
COMPARISON FUNCTION
120
PASS
COPY FUNCTION
122
FAILED

FIGURE 2

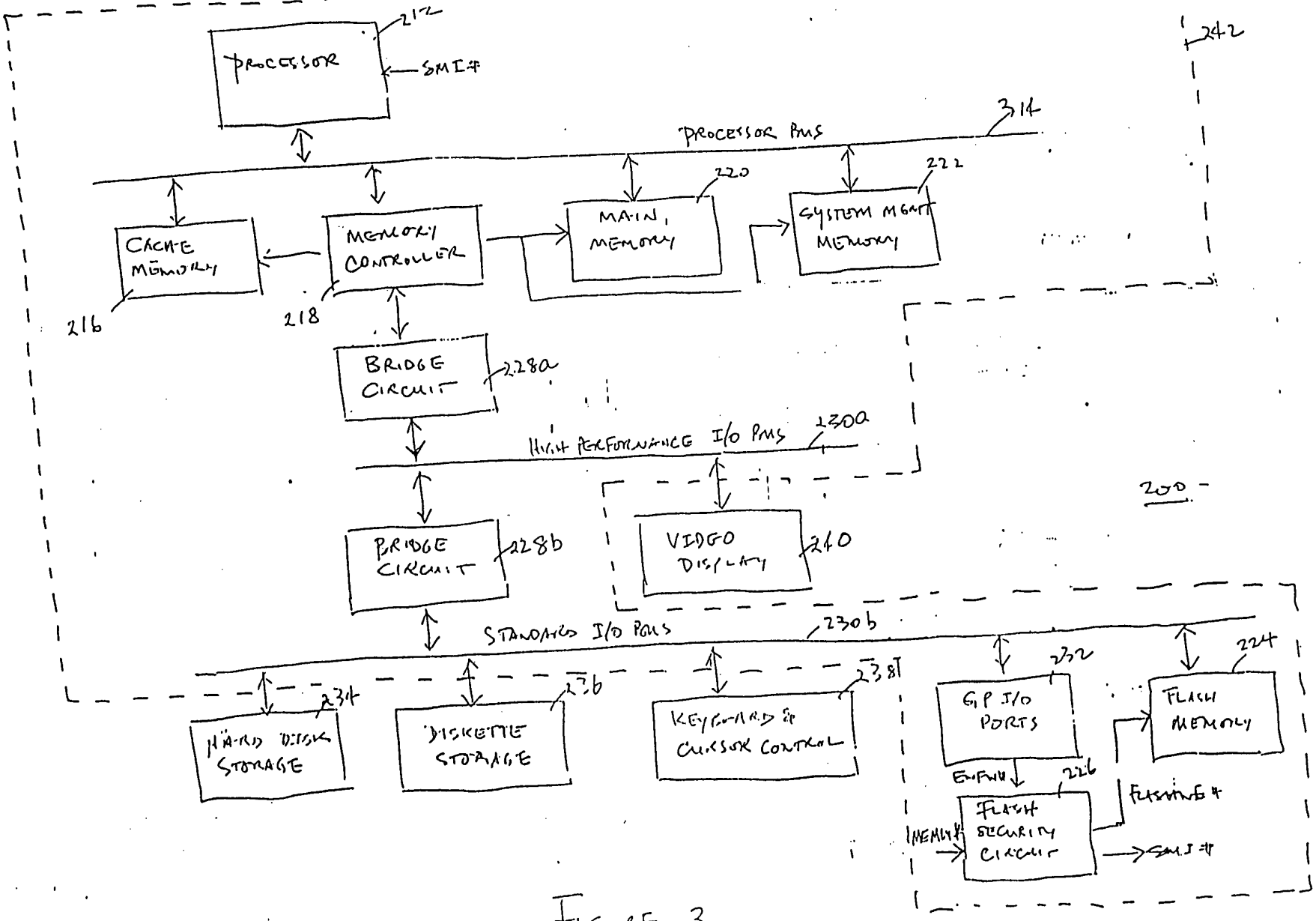

PROCESSOR
212
SMI#
242
PROCESSOR BUS
214
CACHE MEMORY
216
MEMORY CONTROLLER
218
MAIN MEMORY
220
SYSTEM MGMT MEMORY
222
BRIDGE CIRCUIT
228a
HIGH PERFORMANCE I/O BUS
230a
200
BRIDGE CIRCUIT
228b
VIDEO DISPLAY
240
STANDARD I/O BUS
230b
HARD DISK STORAGE
234
DISKETTE STORAGE
236
KEYBOARD & CURSOR CONTROL
238
GP I/O PORTS
232
FLASH MEMORY
224
ENABLE
226
FLASH SECURITY CIRCUIT
FLASHING #
MEMW#
SMI#

FIGURE 3

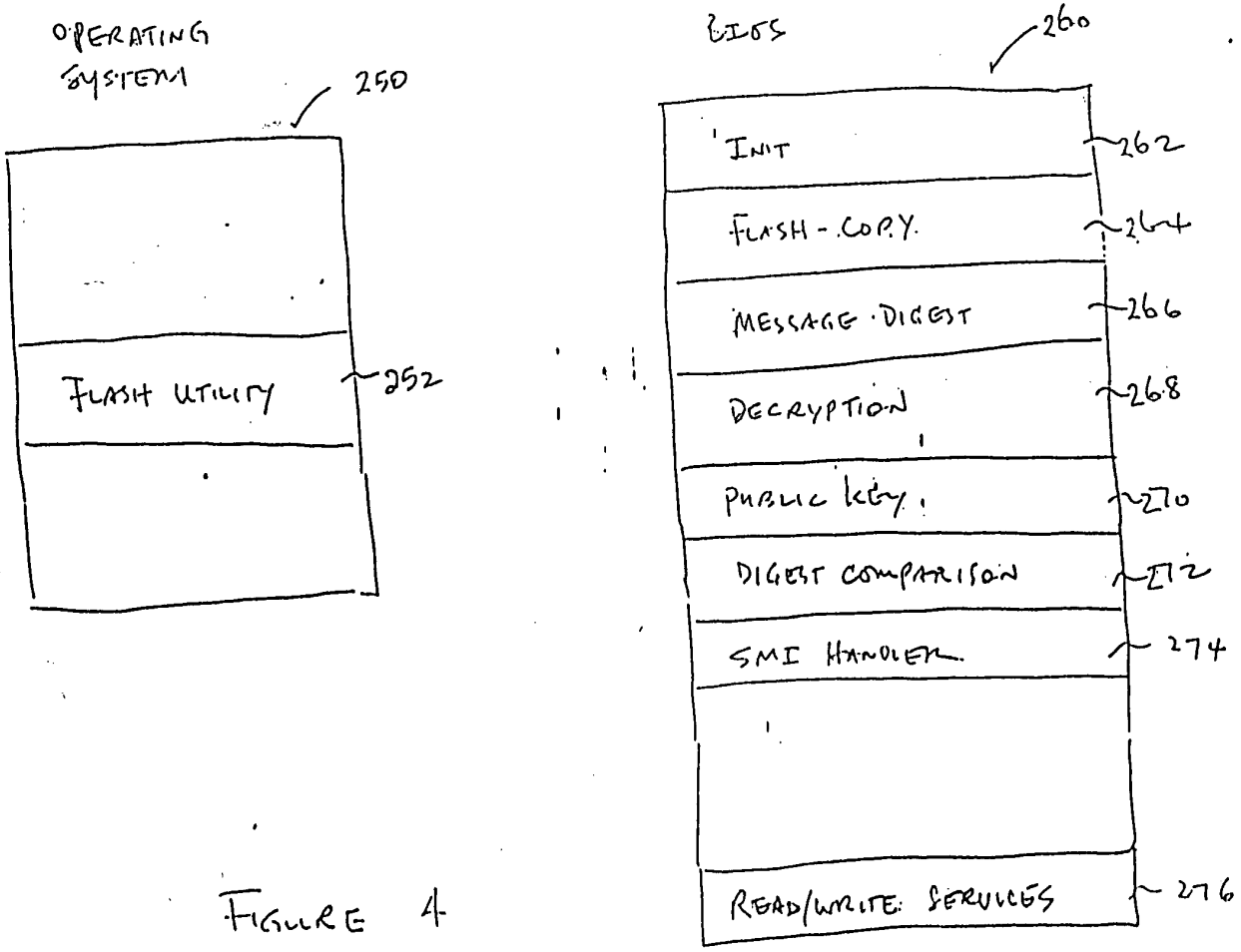

OPERATING SYSTEM
250
FLASH UTILITY
252
BIOS
260
INIT
262
FLASH-COPY
264
MESSAGE DIGEST
266
DECRYPTION
268
PUBLIC KEY
270
DIGEST COMPARISON
272
SMI HANDLER
274
READ/WRITE SERVICES
276

FIGURE 4

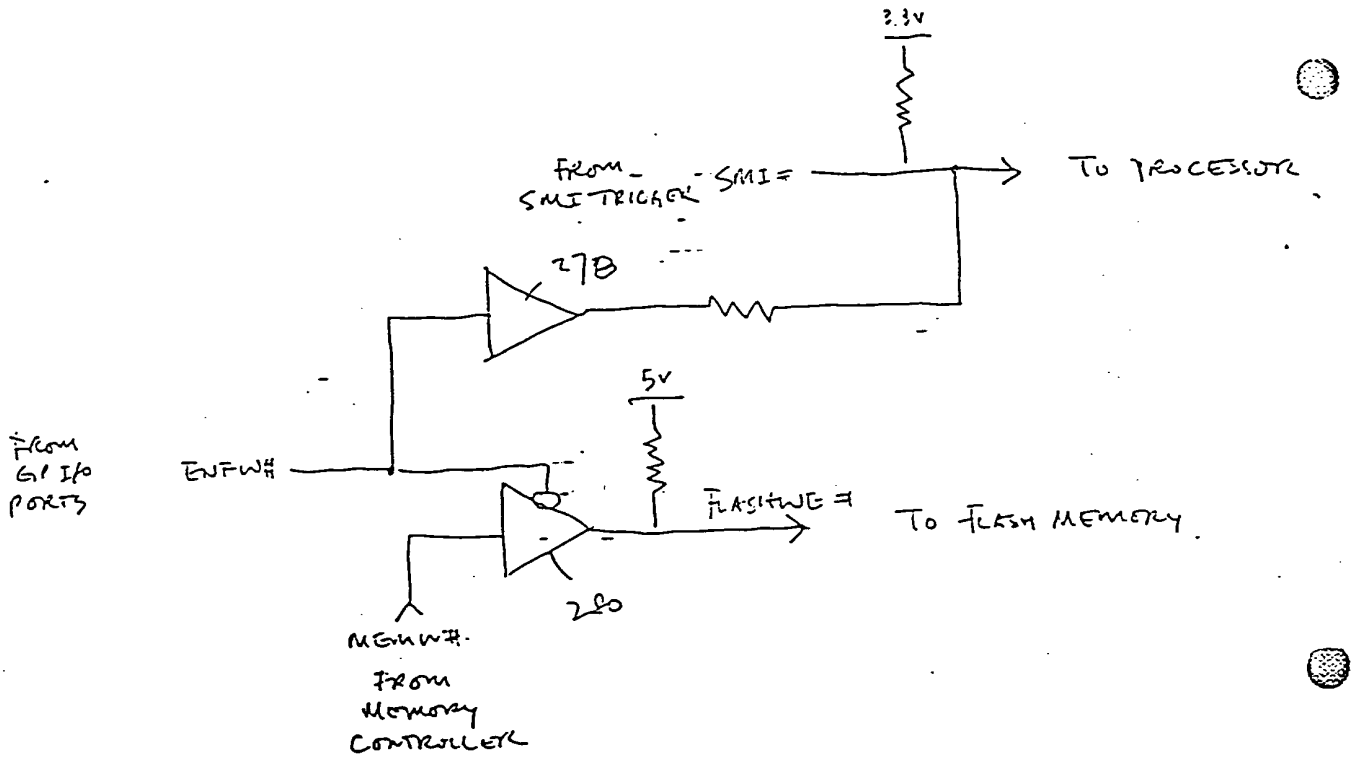

3.3V
FROM SMI TRIGGER
SMI#
TO PROCESSOR
27B
5V
FROM GPIO PORTS
ENFWH#
FLASHWE#
TO FLASH MEMORY
28D
MEMWH#
FROM MEMORY CONTROLLER

FIGURE 5

System Management Mode (Prior Art)

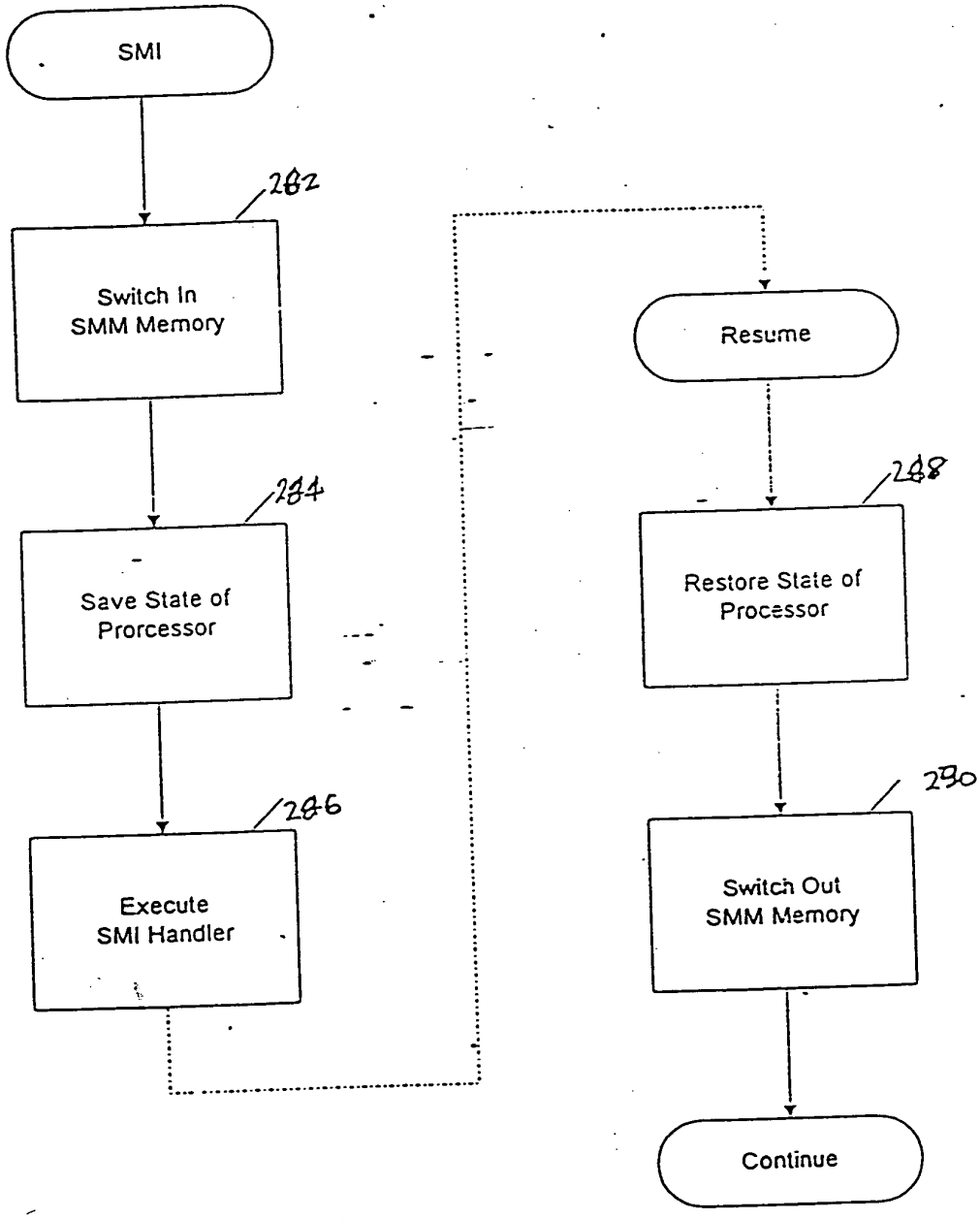


Figure 6

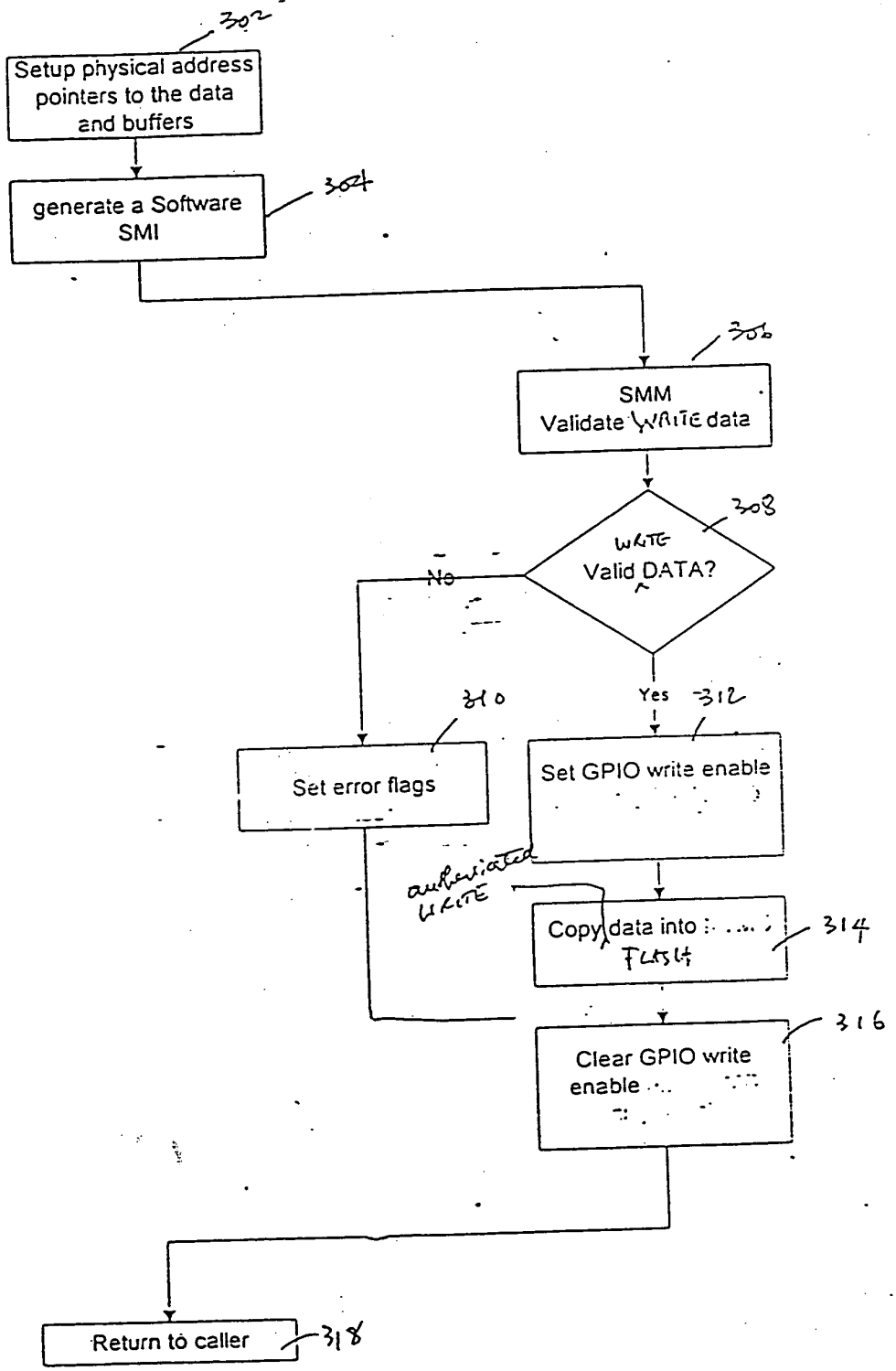

302
Setup physical address pointers to the data and buffers
304
generate a Software SMI
306
SMM Validate WRITE data
308
WRITE Valid DATA?
No
Yes
310
Set error flags
312
Set GPIO write enable
authenticated WRITE
Copy data into FLASH
314
316
Clear GPIO write enable
Return to caller
318

FIGURE 7